(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－331105
（P2001－331105A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
G09C 1/00	640	G09C 1/00	640C	5B017
			640Z	5B049
G06F 12/14	320	G06F 12/14	320A	5J104
17/60	140		140	
	512		512	

審査請求　未請求　請求項の数39　ＯＬ　（全 19 頁）　最終頁に続く

(21)出願番号　特願2000－313122(P2000－313122)
(22)出願日　平成12年10月6日(2000.10.6)
(31)優先権主張番号　特願2000－35631(P2000－35631)
(32)優先日　平成12年2月8日(2000.2.8)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2000－81713(P2000－81713)
(32)優先日　平成12年3月17日(2000.3.17)
(33)優先権主張国　日本（ＪＰ）

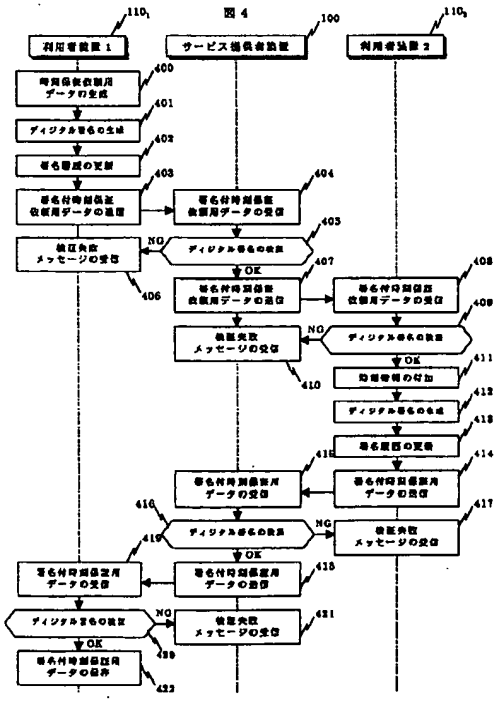
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　宮崎　邦彦
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　情報の保証方法、およびそのシステム

(57)【要約】
【課題】各利用者間で電子文書にディジタル署名を施してやり取りするような環境において、該利用者らがディジタル署名を施した時刻などを簡単に確認可能とする。
【解決手段】利用者装置１１０１は、時刻保証依頼用データをランダムに生成し、該時刻保証依頼用データに対してディジタル署名を施すとともに、自己の署名履歴にその旨追記する。そして、当該署名付時刻保証依頼用データを、サービス提供者装置１００を介して、該サービス提供者装置１００が選択した利用者装置１１０２に送信する。署名付時刻保証依頼用データを受信した利用者装置１１０２は、該署名付時刻保証依頼用データに施されたディジタル署名を検証した後、それに時刻情報を付加してからディジタル署名を施すとともに、自己の署名履歴にその旨追記する。そして、当該署名付時刻保証データを、サービス提供者装置１００を介して利用者装置１１０１に送信する。

図４



1

【特許請求の範囲】

【請求項１】第一と第二の利用者装置を含む複数の利用者装置と、前記複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置とがネットワークを介して情報の受け渡しを行うネットワークサービスシステムで用いられる情報の保証方法であって、

前記第一の利用者装置は、被保証情報を前記サービス提供者装置に送り、

前記サービス提供者装置は、前記複数の利用者装置の中から、第二の利用者装置を選択し、前記第二の利用者装置に被保証情報を送り、

前記第二の利用者装置は、前記被保証情報に署名して、保証情報を生成して保存し、前記保証情報を前記サービス提供者装置に送り、

前記サービス提供者装置は、前記保証情報を、前記第一の利用者装置に送り、

前記第一の利用者装置は、前記保証情報を、前記被保証情報と関連づけて保存する情報の保証方法。

【請求項２】請求項１に記載の情報の保証方法であって、

前記保証情報は、当該保証情報を作成する時刻情報を含む情報の保証方法。

【請求項３】請求項２に記載の情報の保証方法であって、

前記第１の利用者装置は、存在時刻保証対象情報に署名を施し、施した署名と、前記署名の以前、又は以後の時刻情報を持った前記被保証情報とを、時系列を特定可能にして署名履歴に格納し、

前記被保証情報と関連付けて保存された保証情報を用いて、前記第１の利用者装置が署名を施した前記存在時刻保証対象情報の時刻を保証する情報の保証方法。

【請求項４】請求項２に記載の情報の保証方法であって、

前記第１の利用者装置は、前記被保証情報に施した署名と、前記署名の以前、又は以後の時刻情報を持った被保証情報とを、時系列を特定可能にして署名履歴に格納し、

前記保証情報を用いて、前記第１の利用者装置が署名を施した前記被保証情報の時刻を保証する情報の保証方法。

【請求項５】請求項２記載の情報の保証方法において、

前記保証情報が含む時刻情報は、前記第一の利用者装置が前記被保証情報に含めた時刻情報か、または、前記第二の利用者装置が前記保証情報に含めた時刻情報である情報の保証方法。

【請求項６】請求項４に記載の情報の保証方法において、

前記第一の利用者装置は、前記サービス提供者装置から送られてきた、他の利用者装置による被保証情報に対して署名し、前記署名履歴に格納する情報の保証方法。

2

【請求項７】請求項１または３に記載の情報の保証方法において、

前記第一の利用者装置は、被保証情報には前記第一の利用者装置を利用する利用者の署名を含め、

前記第二の利用者装置は、前記送られてきた被保証情報に含まれる署名の正当性を確認し、前記保証情報に、前記第二の利用者装置を利用する利用者の署名を含める情報の保証方法。

【請求項８】第一と第二の利用者装置を含む複数の利用者装置と、前記複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置とがネットワークを介して情報の受け渡しを行うネットワークサービスシステムで用いられる情報の保証方法であって、

前記第一の利用者装置は、前記第一の利用者装置を利用する利用者の署名を施し、時刻情報を含んだ被保証情報を生成し、保存し、

前記第二の利用者装置は、前記サービス提供者装置を介して受け取った、前記被保証情報に、前記第二の利用者装置を利用する利用者の署名を施して保証情報を生成し、保存し、前記第一の利用者装置は、前記サービス提供者装置を介して受け取った前記保証情報を、前記被保証情報と関連づけて保存し、

調停者装置は、前記第二の利用者装置に保存されている保証情報と、前記第一の利用者装置に保存されている前記第二の利用者装置による保証情報とを比較し、前記第一の利用者装置に保存されている署名履歴の署名時刻を特定する情報の保証方法。

【請求項９】請求項８記載の情報の保証方法であって、

前記調停者装置は、前記特定した署名時刻を用いて、前記第１の利用者装置に保存されている署名履歴中の他の被保証情報への署名時刻を特定する情報の保証方法。

【請求項１０】複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを利用する利用者装置における情報の保証方法であって、

前記利用者装置は、被保証情報を当該サービスを提供するサービス提供者装置に送り、

前記サービス提供者装置が選択した他の利用者装置が、前記被保証情報に署名して、生成した、保証情報を、前記サービス提供者装置から受け取り、

前記保証情報を前記被保証情報と関連づけて保存する情報の保証方法。

【請求項１１】請求項１０に記載の情報の保証方法であって、

前記保証情報は、当該保証情報を作成する時刻情報を含む情報の保証方法。

【請求項１２】請求項１１に記載の情報の保証方法であって、

前記利用者装置は、被保証情報に施した署名と、前記署

名の以前、又は以後の時刻情報を持った他の被保証情報とを、時系列を特定可能にして署名履歴に格納し、
前記他の被保証情報に対応する前記保証情報を用いて、前記署名を施した前記被保証情報の時刻を保証する情報の保証方法。
【請求項１３】請求項１２に記載の情報の保証方法において、
前記利用者装置は、前記サービス提供者装置から送られてきた、他の利用者装置による被保証情報に含まれる署名の正当性を確認し、
前記被保証情報に対して、前記利用者装置を利用する利用者の署名を施し、保証情報を生成し、前記署名履歴に格納する情報の保証方法。
【請求項１４】請求項１０に記載の情報の保証方法において、
前記利用者装置は、被保証情報には当該利用者装置を利用する利用者の署名を含め、署名履歴に格納する情報の保証方法。
【請求項１５】複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置が行う情報の受け渡しの仲介方法であって、
前記複数の利用者装置の中から、第二の利用者装置を選択し、第一の利用者装置から送られた被保証情報を、前記第二の利用者装置に送り、前記第二の利用者装置が、前記被保証情報に署名し、生成した保証情報を、前記第一の利用者装置に送る情報の受け渡しの仲介方法。
【請求項１６】第一と第二の利用者装置がネットワークを介して情報の受け渡しを行うネットワークサービスシステムに用いる調停方法であって、
前記第一の利用者装置が生成した、前記第一の利用者装置を利用する利用者の署名を施し、時刻情報を含んだ被保証情報に、前記第二の利用者装置が、前記第二の利用者装置を利用する利用者の署名を施し保存した保証情報と、前記第一の利用者装置が受け取り、前記被保証情報に関連づけて保存した前記保証情報とを入手し、前記入手した保証情報それぞれを比較し、前記記第一の利用者装置に保存されている被保証情報の作成時刻を特定する調停方法。
【請求項１７】利用者装置と、該利用者装置にサービスを提供するサービス提供者装置とからなるネットワークサービスシステムで用いられる署名時刻保証方法であって、
前記サービス提供者装置は、有効期間を持ったチャレンジデータを利用者装置に公開し、
前記利用者装置は、前記チャレンジデータに署名を施して、
前記サービス提供者装置に送信し、
前記サービス提供者装置は、前記有効期間内に利用者装置からチャレンジデータにディジタル署名を施したデータが返送されてきたら、該署名付チャレンジデータを記憶装置に保存する署名時刻保証方法。

【請求項１８】請求項１７記載の署名時刻保証方法であって、
前記利用者装置は、被保証情報に施した署名と、前記署名の以前、又は以後の時刻情報を持った前記署名付きチャレンジデータとを、時系列を特定可能にして署名履歴に格納し、前記利用者装置が署名を施した前記被保証情報の時刻を保証する署名時刻保証方法。
【請求項１９】請求項１８記載の署名時刻保証方法であって、
調停者装置は、前記利用者装置に保存されている被保証情報に施した署名と前記署名付きチャレンジデータと、前記サービス提供者装置に保存されている前記署名付きチャレンジデータとを用いて、前記被保証情報に施した署名時刻を特定する署名時刻保証方法。
【請求項２０】利用者装置と、前記利用者装置に時刻を保証するサービスを提供するサービス提供者装置とからなるネットワークサービスシステムに用いるサービス提供方法であって、
有効期間を持ったチャレンジデータを作成し、前記チャレンジデータを利用者装置に公開し、返送されてきた署名付チャレンジデータが有効期間内にあるかどうかを検証し、有効期間内に返送された該署名付チャレンジデータを記憶装置に保存するサービス提供方法。
【請求項２１】利用者装置と、前記利用者装置に時刻を保証するサービスを提供するサービス提供者装置とからなるネットワークサービスシステムに用いる時刻を保証するサービスの利用方法であって、
前記サービス提供者装置が公開するチャレンジデータに署名を施し、前記署名付チャレンジデータを前記サービス提供者装置に送信し、被保証情報に施した署名と、前記署名の以前、又は以後の時刻情報を持った前記署名付きチャレンジデータとを、時系列を特定可能にして署名履歴に格納するサービス利用方法。
【請求項２２】利用者装置と、前記利用者装置に時刻を保証するサービスを提供するサービス提供者装置とからなるネットワークサービスシステムに用いる調停方法であって、前記利用者装置が、時系列を特定可能にして署名履歴に格納した、被保証情報に施した署名と前記署名の以前、又は以後の時刻情報を持った前記署名付きチャレンジデータと、前記サービス提供者装置に保存されている署名付チャレンジデータを入手し、前記入手した署名付チャレンジデータとを用いて、前記被保証情報に施した署名時刻を特定する調停方法。
【請求項２３】第一と第二の利用者装置を含む複数の利用者装置と、前記複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置とがネットワークを介して情報の受け渡しを行うネットワークサービスシステムであって、
前記第一の利用者装置は、被保証情報を前記サービス提

供者装置に送る送出部と、
前記サービス提供者装置から送られた、保証情報を、前記被保証情報と関連づけて保存する保存部とを備え、
前記サービス提供者装置は、前記複数の利用者装置の中から、第二の利用者装置を選択する選択部と、前記第二の利用者装置に被保証情報を送る送出部と、前記第二の利用者装置から送られた保証情報を、前記第一の利用者装置に送る送出部とを備え、
前記第二の利用者装置は、前記被保証情報に署名して、時刻情報を含む前記保証情報を生成して、保存する保存部と、前記保証情報を前記サービス提供者装置に送る送出部とを備えるネットワークサービスシステム。
【請求項２４】第一と第二の利用者装置を含む複数の利用者装置と、前記複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置とがネットワークを介して情報の受け渡しを行うネットワークサービスシステムであって、
前記第一の利用者装置は、前記第一の利用者装置を利用する利用者の署名を施し、時刻情報を含んだ被保証情報を生成し、保存する生成保存部を備え、
前記第二の利用者装置は、前記サービス提供者装置を介して受け取った、前記被保証情報に、前記第二の利用者装置を利用する利用者の署名を施して保証情報を生成し、保存する生成保存部を備え、
前記第一の利用者装置の前記生成保存部は、前記サービス提供者装置を介して受け取った前記保証情報を、前記被保証情報と関連づけて保存し、
前記調停者装置は、前記第二の利用者装置に保存されている保証情報と、前記第一の利用者装置に保存されている前記第二の利用者装置による保証情報とを入手する入手部と、前記入手した保証情報それぞれを比較する比較部と、前記記第一の利用者装置に保存されている被保証情報の作成時刻を特定する特定部とを備えるネットワークサービスシステム。
【請求項２５】請求項２４記載のネットワークサービスシステムであって、
前記特定部は、前記特定した署名時刻を用いて、前記第１の利用者装置に保存されている署名履歴中の他の被保証情報への署名時刻を特定するネットワークサービスシステム。
【請求項２６】複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを利用する利用者装置であって、
被保証情報を当該サービスを提供する前記サービス提供者装置に送る送出部と、前記サービス提供者装置が選択した他の利用者装置が、前記被保証情報に署名して、生成した、保証情報を、前記サービス提供者装置から受け取る受け取り部と、前記保証情報を、前記被保証情報と関連づけて保存する保存部とを備える利用者装置。
【請求項２７】請求項２６に記載の利用者装置であって、

前記受け取り部は、前記保証情報として、当該保証情報を作成する時刻情報を含む保証情報を受け取る利用者装置。
【請求項２８】請求項２７に記載の利用者装置であって、
被保証情報に施した署名と、前記署名の以前、又は以後の時刻情報を持った被保証情報とを、時系列を特定可能にして署名履歴に格納する格納部を備える利用者装置。
【請求項２９】請求項２８に記載の利用者装置において、
前記サービス提供者装置から送られてきた、他の利用者装置による被保証情報に含まれる署名の正当性を確認する確認部とを備え、
前記格納部は、前記被保証情報に対して、前記利用者装置を利用する利用者の署名を施し、保証情報を生成し、前記署名履歴に格納する利用者装置。
【請求項３０】請求項２６に記載の利用者装置において、
被保証情報には当該利用者装置を利用する利用者の署名を含め、署名履歴に格納する格納部を備える利用者装置。
【請求項３１】複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置であって、
第一の利用者装置から送られた被保証情報を受け取る第一の受け取り部と、前記複数の利用者装置の中から、第二の利用者装置を選択する選択部と、前記被保証情報を、前記第二の利用者装置に送る第一の送出部と、前記第二の利用者装置が、前記被保証情報に署名し、生成した保証情報を受け取る第二の受け取り部と、前記受け取った保証情報を、前記第一の利用者装置に送る第二の前記送出部を備える情報の受け渡しを仲介するサービスを提供するサービス提供者装置。
【請求項３２】第一と第二の利用者装置がネットワークを介して情報の受け渡しを行うネットワークサービスシステムに用いる調停者装置であって、
前記第一の利用者装置が生成した、前記第一の利用者装置を利用する利用者の署名を施し、時刻情報を含んだ被保証情報に、前記第二の利用者装置が、前記第二の利用者装置を利用する利用者の署名を施し保存した保証情報と、前記第一の利用者装置が受け取り、前記被保証情報に関連づけて保存した前記保証情報とを入手する入手部と、前記入手した保証情報それぞれを比較する比較部と、前記記第一の利用者装置に保存されている被保証情報の作成時刻を特定する特定部とを備える調停者装置。
【請求項３３】利用者装置と、該利用者装置にサービスを提供するサービス提供者装置とからなるネットワークサービスシステムであって、
前記サービス提供者装置は、有効期間を持ったチャレン

ジデータ作成する作成部と、前記チャレンジデータを利用者装置に公開する公開部と、返送されてきた署名付チャレンジデータが有効期間内にあるかどうかを検証する検証部と、有効期間内に返送された該署名付チャレンジデータを記憶装置に保存する保存部とを備え、
前記利用者装置は、前記チャレンジデータに署名を施す署名部と、前記署名付チャレンジデータを前記サービス提供者装置に送信する送信部とを備えるネットワークサービスシステム。

【請求項３４】請求項３３記載のネットワークサービスシステムは、調停者装置を備え、
前記調停者装置は、前記利用者装置が、時系列を特定可能にして署名履歴に格納した、被保証情報に施した署名と、前記署名の以前、又は以後の時刻情報を持った前記署名付きチャレンジデータと、を入手する入手部と、前記サービス提供者装置に保存されている署名付チャレンジデータを入手する入手部と、前記入手した署名付チャレンジデータとを用いて、前記被保証情報に施した署名時刻を特定する特定部とを備えるネットワークサービスシステム。

【請求項３５】利用者装置と、該利用者装置にサービスを提供するサービス提供者装置とからなるネットワークサービスシステムに用いるサービス提供者装置であって、
有効期間を持ったチャレンジデータを作成する作成部と、
前記チャレンジデータを利用者装置に公開する公開部と、
返送されてきた署名付チャレンジデータが有効期間内にあるかどうかを検証する検証部と、
有効期間内に返送された該署名付チャレンジデータを記憶装置に保存する保存部と、を備えるサービス提供者装置。

【請求項３６】利用者装置と、該利用者装置にサービスを提供するサービス提供者装置とからなるネットワークサービスシステムに用いる利用者装置であって、
前記利用者装置は、前記サービス提供者装置が公開するチャレンジデータに署名を施す署名部と、前記署名付チャレンジデータを前記サービス提供者装置に送信する送信部と、被保証情報に施した署名と、前記署名の以前、又は以後の時刻情報を持った前記署名付きチャレンジデータとを、時系列を特定可能にして署名履歴に格納する格納部とを備える利用者装置。

【請求項３７】利用者装置と、該利用者装置にサービスを提供するサービス提供者装置とからなるネットワークサービスシステムに用いる調停者装置であって、
前記利用者装置が、時系列を特定可能にして署名履歴に格納した、被保証情報に施した署名と前記署名の以前、又は以後の時刻情報を持った前記署名付きチャレンジデータと、前記サービス提供者装置に保存されている署名付チャレンジデータとを入手する入手部と、前記入手した署名付チャレンジデータとを用いて、前記被保証情報に施した署名時刻を特定する特定部とを備える調停者装置。

【請求項３８】第一の利用者装置と、前記第一の利用者装置にサービスを提供するサービス提供者装置とからなり、前記第一の利用者装置が作成した署名時刻を保証するサービスを提供するネットワークサービスシステムで用いられる情報の保証方法であって、
前記第一の利用者装置自身または、他の利用者装置による署名を用いて、前記署名時刻の保証を行なう情報の保証方法。

【請求項３９】第一と第二の利用者装置を含む複数の利用者装置と、前記複数の利用者装置間で行われる情報の受け渡しを仲介するサービスを提供するサービス提供者装置とに、ネットワークを介した情報の受け渡しを行うネットワークサービスシステムを行なわせるプログラムを記憶した媒体であって、
前記第一の利用者装置に、被保証情報を前記サービス提供者装置に送らせ、前記サービス提供者装置から送られた保証情報を、前記被保証情報と関連づけて保存させ、前記サービス提供者装置に、前記複数の利用者装置の中から、第二の利用者装置を選択させ、前記第二の利用者装置に被保証情報を送らせ、前記第二の利用者装置から送られた保証情報を、前記第一の利用者装置に送らせ、前記第二の利用者装置に、前記被保証情報に署名させ、保証情報を生成させ、保存させ、前記保証情報を前記サービス提供者装置に送らせるプログラムを記憶した媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、マルチメディアデータの正当性を保証する技術に関する。

【０００２】

【従来の技術】様々な情報が電子化され、ネットワークを介してやり取りされる情報システムが構築されつつある。電子化された情報の利用に際しては、　第三者に盗聴される、　第三者に改ざんされる、　相手が自称する本人でない（第３者になりすまされる）、などといった危険がある。

【０００３】これらの危険から情報システムを守るために、セキュリティ技術が広く用いられている。前記　に対しては通信データを暗号化する。また、前記　、　に対しては通信データにディジタル署名を施す。

【０００４】ディジタル署名技術の概要については、例えば「Ｃｒｙｐｔｏｇｒａｐｈｙａｎｄ　Ｄａｔａ　Ｓｅｃｕｒｉｔｙ（著者：Ｄｏｒｏｔｈｙ　Ｅｌｉｚａｂｅｔｈ　Ｒｏｂｌｉｎｇ　Ｄｅｎｎｉｎｇ、発行所：ＡＤＤＩＳＯＮ－ＷＥＳＬＥＹ　ＰＵＢＬＩＳＨＩＮＧ　ＣＯＭＰＡＮＹ）」の１４ページから１６ページに記載

されている。

【０００５】上記ディジタル署名技術がビジネスの世界でも利用されはじめており、従来の印鑑やサインの代わりにディジタル署名を用いた上で、申請文書や契約文書等を電子化するシステムが開発されている。ディジタル署名が施された電子文書にはある一定期間保存される必要があるものも多い。例えば、電子化された債権約束手形等が換金されるのは、あらかじめ決められた期間が過ぎた後なので、それまで安全に保存しておくことが必要である。その期間の間に、それら電子文書の作成者の秘密鍵が漏洩した場合には、該電子文書が正当なものであるか、あるいは偽造されたものであるかということが判別できなくなってしまう。

【０００６】そのため、上記システムにおいては、各利用者は、どの電子文書に対してディジタル署名を施したかということを事後になって確認することが可能な署名履歴を保存するようにしている。この署名履歴は、自己の正当性、すなわち、自分が署名した覚えのない電子文書が持ちこまれた場合に当該電子文書が偽造されたものであることを証明するためや、自分が署名した電子文書の正当性を証明するためとして用いるものである。

【０００７】一方、各種のネットワークシステムでは、各利用者に関係する様々な情報の正当性を、利用者にとって、中立の立場にある、あるいは、信頼されるべき立場にある第三者機関に保証してもらうようなことも行われている。

【０００８】例えば、公開鍵暗号方法を利用したシステムにおいて、各利用者が所有する公開鍵の正当性は、認証局と呼ばれる第三者機関が利用者の識別情報や公開鍵を含んだ情報にディジタル署名を施すことによって保証する。また、電子的に契約文書等を取り交わすようなケースにおいて、該電子契約文書が取り交わされた時刻や内容、あるいは契約行為が行われたという事実そのものの正当性は、タイムスタンプオーソリティと呼ばれる第三者機関がタイムスタンプ（時刻情報等にディジタル署名を施したデータ）を当該電子契約文書に付加したり、公証局と呼ばれる第三者機関が当該電子契約文書に署名したりすることによって保証する。

【０００９】これらの方法については、例えば、「ＳＥＣＵＲＥ　ＥＬＥＣＴＲＯＮＩＣＣＯＭＭＥＲＣＥ（著者：Ｗａｒｗｉｃｋ　Ｆｏｒｄ、Ｍｉｃｈａｅｌ　Ｓ．Ｂａｕｍ、発行所：Ｐｒｅｎｔｉｃｅ　Ｈａｌｌ　ＰＴＲ）」の１９３ページから２６１ページ、「ＣＲＹＰＴＯＧＲＡＰＨＹ　Ｔｈｅｏｒｙ　ａｎｄ　Ｐｒａｃｔｉｃｅ（著者：Ｄｏｕｇｌａｓ　Ｒ．Ｓｔｉｓｏｎ、発行所：ＣＲＣ　Ｐｒｅｓｓ）」の２５４ページから２５５ページや、特開平１０－３２７１４７号公報に開示されている。

【００１０】

【発明が解決しようとする課題】第三者機関に各種情報の正当性を保証してもらうシステムでは、該第三者機関自身のディジタル署名が偽造されないことが前提となっている。しかし、公開鍵暗号方法の場合、公開鍵が利用者に公開されているため、対応する秘密鍵を算出することは基本的に可能であり、時間の経過にしたがってその危険性が増していく。第三者機関自身の秘密鍵が漏洩してしまった場合には、当該第三者機関のディジタル署名の偽造が可能となるため、情報の正当性が保証されなくなる。例えば、取引相手が本人であるかどうか確認できなくなってしまったり、当該システムを利用して作成された契約文書等に付されたタイムスタンプが過去に遡って信用できないものとなってしまい、被害が大きい。

【００１１】電子的な契約文書等、各種情報を取り交わすようなケースにおいて、第三者機関に各種情報の正当性を保証してもらうために、その都度、第三者機関に当該情報を送信してタイムスタンプを押してもらったり署名してもらったりするシステムでは、第三者機関に負荷が集中し、処理が遅くなるおそれがある。

【００１２】本発明は、上記課題を解決するためになされたものであり、本発明の目的は、システムの利用者にサービスを提供するサービス提供者と利用者とからなるネットワークシステムにおいて、より高い安全性を持つ情報の正当性の保証方法、または、サービス提供者にかかる負荷が少ない情報の正当性の保証方法を提供することにある。

【００１３】本発明の他の目的は、各利用者が、上記方法を用いて過去に作成した情報の検証方法と、作成した情報に関して生じた問題を、当該関係者、あるいは該関係者に依頼を受けて調停作業を行う第三者（調停者）が調停する方法を提供することにある。

【００１４】本発明のさらなる目的は、上記方法を用いたサービスシステムや、そこで用いる利用者装置やサービス提供者装置または調停者装置、または、それらを機能的に実現するプログラム（コード、モジュール、ユニットともいう）を提供することにある。

【００１５】

【課題を解決するための手段】上記目的を達成するために、本発明は、システムの利用者にサービスを提供するサービス提供者と利用者とからなるネットワークシステムにおいて、サービス提供者にシステム全体の安全性に影響する秘密情報を持たせずに、情報の正当性を保証する技術を提供する。

【００１６】より具体的には、本発明は、

（１）当サービスを利用する他の利用者が情報の正当性を保証する技術

（２）情報の正当性を保証するためにサービス提供者が管理する情報には公開性を持たせながら情報の正当性を保証する技術

とを提供する。

【００１７】上記(１)は、具体的には、ネットワークに

接続された複数の利用者装置と、前記複数の利用者装置間で行われる情報の受け渡しの仲介サービスを提供するサービス提供者装置とからなるネットワークサービスシステムで用いられる情報の保証方法であって、以下のように実施する。

【００１８】・利用者装置１は、サービス提供者装置に被保証情報を送る。

【００１９】・サービス提供者装置は、被保証情報を、利用者装置１以外の任意に(無作為に)選択した利用者装置２に対して送信する。

【００２０】・利用者装置２は、相互扶助、すなわち、自己がサービスを受けようとするときに他利用者装置に協力してもらうために、他利用者装置から依頼を受けた場合に協力するという考え方を前提として、サービス提供者装置から送られてきた被保証情報に対して自己の署名を施した保証情報を生成し、サービス提供者装置に返送する。

【００２１】・サービス提供者装置は、利用者装置２から送られてきた保証情報を利用者装置１に転送する。

【００２２】この方法に従えば、利用者装置１は、自らの署名履歴に格納した、保証してもらいたい情報に対する、他の利用者の署名を得ることができるので、上記情報が保証される。また、上記保証行為は主に利用者装置が行なうので、サービス提供者を介さずに、複数の利用者装置間で行われてもかまわない。

【００２３】より具体的には、以下のように実施する。

【００２４】・利用者装置１は、時刻保証依頼用データに署名を施した被保証情報(保証対象情報ともいう)、すなわち、署名付時刻保証依頼用データを作成し、自らの署名履歴の中に保存したのち、サービス提供者装置に送信する。

【００２５】・サービス提供者装置は、利用者装置１から送られてきた署名付時刻保証依頼用データを、利用者装置１以外の任意に選択した利用者装置２に対して送信する。

【００２６】・利用者装置２は、受け取った署名付時刻保証依頼用データに時刻情報を付加した後、署名を施して、保証情報すなわち署名付時刻保証データを生成し、自らの署名履歴の中に保存したのち、サービス提供者装置を介して利用者装置１に送る。

【００２７】・利用者装置１は、時刻情報が含まれた署名付時刻保証データを、対応する時刻保証依頼用データ等と関連づけて保存する。

【００２８】この方法に従えば、利用者装置１は、自らの署名履歴に、時刻を保証してもらいたい他の署名(例えば、電子契約文書などへの署名)を格納すると共に、その前又は後の時刻情報を持った署名付時刻保証依頼用データを格納することにより、上記他の署名の時刻が保証される。

【００２９】加えて、この方法に従えば、利用者装置１の署名履歴と利用者装置２の署名履歴との間に履歴情報の交差が生じる。利用者装置２においても同様の処理を行なうと、利用者装置１の署名時刻を保証するための証拠が、さらに拡散して保管される。これにより、情報を偽造しようとするときの作業量が鼠算的に拡大し、かつ、偽造作業を行うためには複数の利用者、または複数の利用者装置を巻き込むことが必要となるため、不正を抑止する大きな効果が得られる。

【００３０】また、上記(２)を、以下のように実施する。

【００３１】・サービス提供者装置は、チャレンジデータを作成し、ある決められた期間、利用者装置に対して公開する。チャレンジデータとは、後からそれが生成された時刻あるいは期間を特定できるように、さらに、公開前には、他のチャレンジデータなど、他の情報から予測できないように作成する情報のことで、定期または不定期に変更する乱数を用いたり、所定の規則で作成したりする。後に時刻情報など特定するための情報または規則は、サービス提供者装置が保存しておく。チャレンジデータを事前に知ることができないように作成することにより、署名時刻が保証できる。

【００３２】・利用者装置は、サービス提供者装置が公開しているチャレンジデータを取得して署名を施し、署名付チャレンジデータを自装置の署名履歴の中に保存する。保存後、該署名付チャレンジデータをサービス提供者装置に送信する。

【００３３】・サービス提供者装置は、決められた期間内に、利用者装置から署名付チャレンジデータを受信した場合に、それを保存する。

【００３４】この方法に従えば、利用者装置は、自らの署名履歴に、時刻を保証してもらいたい他の署名(例えば、電子契約文書などへの署名)を格納すると共に、その前又は後の時刻情報を持った署名付チャレンジデータを格納することにより、上記他の署名の時刻が保証される。

【００３５】本発明によれば、利用者が署名を施した情報、たとえば日時を保証するための、より安全なサービスを提供することができる。この方法では、サービス提供者装置は、システム全体の安全性に影響するような秘密情報を管理することがないので、より安全である。また、負荷が少ない簡単な手順でサービス提供者装置が運用されるので、サービス提供時の処理速度が低下するおそれが少ない。

【００３６】本発明において、署名を施すということは、本人だけが知っているあるいは提出できる筈の秘密情報を用いて、対象のものを保証する情報を作成すること、またはその対象のものに添付することを意味する。その実現方法の一つが、上記文献が開示する公開鍵暗号によるディジタル署名技術である。なお施された署名には、保証対象のものが含まれる場合と含まれない場合と

がある。

【００３７】また、上記被保証情報とは、氏名や住所などといった属性情報や、該利用者の所有物に関する情報、あるいは、該利用者の行為に関する情報を指す。

【００３８】また、本発明では、時刻として、年、月、日、曜日なども特定できる情報を含む場合もある。

【００３９】

【発明の実施の形態】以下、本発明を電子文書への署名時刻の保証に適用した例について、説明する。各図面において、同一の番号は同様の部品・要素・処理を表すものとする。

【００４０】（実施例１）図１は本発明が適用されたネットワークサービスシステムの概略構成図である。

【００４１】本実施形態のネットワークサービスシステムは、図１に示すように、サービス提供者装置１００と利用者装置１１０_{1}～１１０_{N}（以下、単に利用者装置１１０とも称する）が、ネットワーク１２０を介して、互いに接続されて構成されている。

【００４２】サービス提供者装置１００は、サービス提供者１３０が使用する装置であり、利用者装置１１０に対して、後述のサービスを提供する。

【００４３】利用者１４０_{1}～１４０_{N}（以下、単に利用者１４０とも称する）は、利用者装置１１０を介して、サービス提供者装置１００が提供するサービスを受けることができる。サービス提供者装置１００および利用者装置１１０間のデータのやり取りは、ネットワーク１２０を介して行われる。

【００４４】サービス提供者１３０は、本発明のネットワークサービスシステムの利用者が信頼する第三者である。利用者１４０は、システムを利用する一般の人であり、少数の利用者は利益を得るためなどの目的により不正行為を働く可能性はあるが、大多数の利用者は不正行為を働くことはないと仮定する。

【００４５】次に、本実施形態のネットワークサービスシステムを構成するサービス提供者装置１００および利用者装置１１０のハードウェア構成、ソフトウェア構成について、図面を参照して説明する。

【００４６】図２は、サービス提供者装置１００および利用者装置１１０のハードウェア構成を示す図である。

【００４７】サービス提供者装置１００では、入力装置２０１と、表示装置２０２と、中央処理装置（ＣＰＵ）２０３と、メモリ２０４と、通信処理装置２０５と、記憶装置２０６とが、バス２００によって互いに接続されている。利用者装置１１０では、さらに、署名処理装置２０７が、接続されている。

【００４８】入力装置２０１は、サービス提供者装置１００あるいは利用者装置１１０の使用者がデータやコマンドなどを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【００４９】表示装置２０２は、上記利用者にメッセージなどを表示するために用いられるものであり、ＣＲＴや液晶ディスプレイなどで構成される。

【００５０】ＣＰＵ２０３は、上記各構成要素を統括的に制御したり、様々な演算を行う。

【００５１】メモリ２０４は、ＣＰＵ２０３が上記の処理を実行するために必要なプログラムや、データなどを一時的に記憶するために用いられるものである。

【００５２】通信処理装置２０５は、ネットワーク１２０を介したデータのやり取りを行うために用いられる。

【００５３】記憶装置２０６は、使用されるプログラムやデータなどを永続的に記憶するために用いられるものであり、ハードディスクやフロッピー（登録商標）ディスクなどで構成される。記憶装置２０６には、後の調停作業において、保証情報を作成してもらった他の利用者を特定するための情報が格納されているので、そのデータが失われないような手段を講じる。たとえば、不揮発性の記憶媒体を用いることや、定期的にバックアップを作成することが有効である。また、利用者装置１１０を交換する場合には、記憶装置２０６の内容を移すことも必要である。

【００５４】署名処理装置２０７は、利用者装置１１０において、ディジタル署名に使用される利用者１４０の秘密鍵や公開鍵、あるいは署名履歴などを記憶したり、該秘密鍵を用いてディジタル署名を生成したりするためなどに用いられるものである。

【００５５】該署名処理装置２０７に記憶されたデータは、利用者１４０も含めて誰にも改ざんや削除などができないように保護されている。具体的には、秘密鍵は、利用者１４０にも知られないように、外部から読み出せないような手段を講じた上で署名処理装置２０７に格納されているものとする。秘密鍵を利用者１４０が知ると、署名処理装置２０７以外の装置を用いた署名の偽造が可能になるためである。署名履歴は、自分が署名した覚えのない電子文書が持ちこまれた場合に、自己の正当性、すなわち、当該電子文書が偽造されたものであることを証明するためや、ある電子文書に自分が署名したことを証明するためとして用いる。そのため、利用者１４０自身も署名履歴を改変できないようにしておく。たとえば１回だけ書き込み可能なメモリを用いることで実現できる。こうした構成により、特定の公開鍵に対応した署名履歴は、特定の署名処理装置２０７に残ることになり、後の調停作業において有効になる。

【００５６】署名処理装置２０７は、例えばＩＣカードのように、利用者装置１１０から切り離すことができるものが望ましい。この場合は、署名処理装置２０７は、ＣＰＵと、ＣＰＵを動作させるプログラムや署名履歴を格納する記憶装置と、利用者装置との情報のやり取りを行なうインタフェース装置とを備える。また、署名を生成するための専用の演算装置（ハードウェア）を備えても良い。同じく、利用者装置１１０にもインタフェース

装置を付加する。切り離し可能な構成にすると、複数の利用者が各利用者装置１１０を共有できるようになり、便利である。この場合、記憶装置２０６中には、複数の利用者による署名処理の記録が残ることになる。

【００５７】また、署名処理装置２０７を持ち運び可能とすることで、署名行為を行なう場所を制限されることがない。

【００５８】図３は、サービス提供者装置１００および利用者装置１１０が具備するメモリ２０４のソフトウェア構成を示す図である。

【００５９】図３(ａ)は、サービス提供者装置１００のソフトウェア構成を示す図であり、オペレーティングシステム（ＯＳ）３００と、通信プログラム３０１と、サービス提供プログラム３０２とからなる。図３(ｂ)は、利用者装置１１０のソフトウェア構成を示す図であり、オペレーティングシステム（ＯＳ）３００と、通信プログラム３０１と、サービス利用プログラム３０２と、電子文書処理プログラム５０３と、セキュリティプログラム５０４とからなる。

【００６０】ＯＳ３００は、サービス提供者装置１００、あるいは利用者装置１１０全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現する。

【００６１】通信プログラム３０１は、以下に説明するサービス提供プログラム３０２や、サービス利用プログラム３０３の制御により、サービス提供者装置１００と利用者装置１１０、あるいは各利用者装置１１０の間でデータのやり取りを行う。以下の説明では、通信プログラム３０１の動作は明示しない。

【００６２】サービス提供プログラム３０２は、サービス提供装置１００において、利用者装置１１０に対して後述のサービスを提供する際に必要な処理を制御する。

【００６３】サービス利用プログラム３０３は、利用者装置１１０において、サービス提供者装置１００が提供するサービスを利用する際に必要な処理、あるいはサービス提供者装置１００からの依頼に基づく処理を制御する。

【００６４】電子文書処理プログラム３０４は、利用者装置１１０において、各利用者装置間でやり取りされる申請文書や契約文書などといった、保証対象となる電子文書の処理（作成、閲覧等）を制御する。

【００６５】セキュリティプログラム３０５は、利用者装置１１０において、署名処理装置２０７と連携し、各利用者装置間でやり取りされる上記電子文書や各種データに対してディジタル署名を施したり、電子文書に施されたディジタル署名を検証したり、署名履歴を保存したりする処理を制御する。

【００６６】本実施形態のネットワークサービスシステムが提供する署名時刻保証方法の手順とその利用について、図面を参照して説明する。以下の例は、各利用者が利用者装置を操作し、他の利用者との間でディジタル署名を施した電子契約文書をやり取りする個々の契約手続きの合間に、この署名時刻保証方法を利用することにより、個々の契約手続が行なわれた時刻を証明するものである。なお、本発明によれば、契約手続きが行われた時刻に限らず、より一般に、さまざまな電子文書に対する利用者の署名時刻を証明することが可能である。すなわち、さまざまな電子文書が作成後どれだけ時間が経過したかを証明すること（経時証明）が可能である。したがって、各利用者は、保持あるいは作成した電子文書の存在時刻証明をしたい場合には、自分自身で、本発明にしたがって、当該電子文書に対し署名をほどこすことにより、署名生成時点に当該電子文書が存在していたことを証明することが可能となる。これは、特許アイデアや著作権の先行性を示したい場合などには、特に有効である。さらに、この方法によれば、存在時刻証明をしたい対象となる電子文書自体は他人に預託しなくても、当該文書の存在時刻証明をすることが可能である。

【００６７】図５は、署名処理装置２０７に設けた署名履歴を例示する図である。例えば、図５の署名対象データの欄に示すＦとの電子契約文書を作成するとき、当該文書に施したディジタル署名を施した時刻を保証するためには、その署名を作成して履歴に保存する前後に、１５番の時刻保証依頼用データ２、１８番の時刻保証依頼用データ３へ署名して、それぞれ前時刻保証データ、後時刻保証データを作成して履歴に保存し、電子契約文書への署名時刻を保証する。署名履歴に格納された各情報の時系列は、以前の履歴またはその特徴値を含めたうえで署名する等の方法により、保証できる。

【００６８】図４は、利用者１４０_{1}が、サービス提供者１３０が提供するサービスを受ける場合、すなわち、時刻保証データを作成する際の、サービス提供者装置１００、利用者装置１１０_{1}、および利用者装置１１０_{2}の動作を説明するための図である。

【００６９】利用者装置１１０_{1}において、サービス利用プログラム３０３の制御により、セキュリティプログラム３０５は、時刻保証依頼用データをランダムに生成し（ステップ４００）、該時刻保証依頼用データを記憶装置２０６に格納するとともに、該時刻保証依頼用データにディジタル署名を施し（ステップ４０１）、署名履歴の中に、該時刻保証依頼用データとそのディジタル署名からなる署名付き時刻保証依頼用データを追記する（ステップ４０２）。サービス利用プログラム３０３は、当該署名付時刻保証依頼用データをサービス提供者装置１００に送信する（ステップ４０３）。

【００７０】サービス提供者装置１００において、サービス提供プログラム３０２は、署名付時刻保証依頼用データを受信する（ステップ４０４）。サービス提供プログラム３０２は、ディジタル署名の検証を行い（ステップ４０５）、ディジタル署名が正しく検証できなかった

場合には、検証失敗メッセージを利用者装置１１０$_1$に送信する（ステップ４０６）。正しく検証できた場合には、該署名付時刻保証依頼用データを、利用者装置１１０$_1$以外の任意に(無作為に)選択した利用者装置１１０$_2$に送信する（ステップ４０７）。ステップ４０５の検証処理は省略してもよい。

【００７１】利用者装置１１０$_1$が検証失敗メッセージを受け取った場合には、ステップ４００から再度行う。サービスの利用をやめる場合には、そのまま処理を終了してもよい。

【００７２】利用者装置１１０$_2$において、サービス利用プログラム３０３は、署名付時刻保証依頼用データを受信し（ステップ４０８）、セキュリティプログラム３０５は、ディジタル署名の検証を行う（ステップ４０９）。ディジタル署名が正しく検証できなかった場合には、サービス利用プログラム３０３は、検証失敗メッセージをサービス提供者装置１００に送信する（ステップ４１０）。正しく検証できた場合に、署名処理装置２０７は、サービス利用プログラム３０３の制御の下、セキュリティプログラム３０５と連携して、受け取った署名付時刻保証依頼用データに時刻情報を付加し（ステップ４１１）、ディジタル署名を施し（ステップ４１２）、図５に示すものと同様の署名履歴に、時刻情報を付加した該署名付き時刻保証依頼用データとそのディジタル署名からなる署名付き時刻保証データを１７番、１９番のように追記する（ステップ４１３）。このように、利用者装置１１０$_2$で追記される署名履歴は、時刻保証依頼用データではなく利用者装置１１０$_1$による署名付時刻保証依頼用データが署名対象データとなる点が異なっている。

【００７３】これら利用者装置１１０$_2$での処理は、基本的には他人、すなわち、利用者装置１１０$_1$の利用者のために行なわれるものである。しかし、同時に、自らの署名処理装置の署名履歴の中に、他人の署名によって保証される時刻情報を含めることにもなり、利用者装置１１０$_2$の利用者にとっても、その署名を行なった前後の行為を特定する時刻が保証されることになり、利益がある。

【００７４】さらに、このように自己の署名履歴を他者の署名履歴と交差させることは、当該署名が確かに行われたという証拠を分散して持つことに他ならず、署名そのものを偽造しようとしたり、署名が施された時刻情報を改変しようとしたりするときの作業量を増大させ、かつ、それら不正を行うために複数の利用者、または複数の利用者装置を巻き込む必要がある。このように、不正を抑止する大きな効果が得られるため、利用者装置１１０$_1$の利用者および利用者装置１１０$_2$の利用者双方にとって有益である。

【００７５】さらに、利用者間で署名履歴を交差させる処理を適宜実行すれば、図１０に示すように、システムの全利用者の署名履歴が複雑に絡み合った状態になり、全ての署名履歴の信頼性を高めることにもなる。

【００７６】そのあと、サービス利用プログラム３０３は、作成した署名付時刻保証データをサービス提供者装置１００に送信する（ステップ４１４）。ステップ４１０の検証処理は省略してもよい。サービス提供者装置１００が検証失敗メッセージを受け取った場合には、当該署名付時刻保証依頼用データを利用者装置１１０$_2$に再送する。

【００７７】署名付時刻保証データを受信した（ステップ４１５）サービス提供プログラム３０２は、ディジタル署名の検証を行う（ステップ４１６）。ディジタル署名が正しく検証できなかった場合には、検証失敗メッセージを利用者装置１１０$_2$に送信する（ステップ４１７）。正しく検証できた場合には、該署名付時刻保証データを利用者装置１１０$_1$に送信する（ステップ４１８）。同時に複数の利用者装置１１０からサービス提供依頼を受けている場合には、当該署名付時刻保証データがどの署名付時刻保証依頼用データに対応したものであるかを確認することによって、署名付時刻保証データを返送する利用者装置１１０を選択する。ステップ４１６の検証処理は省略してもよい。利用者装置１１０$_2$が検証失敗メッセージを受け取った場合には、サービス利用プログラム３０３は、当該署名付時刻保証データをサービス提供者装置１００に再送する。

【００７８】利用者装置１１０$_1$において、サービス利用プログラム３０３は、署名付時刻保証データを受信し（ステップ４１９）、セキュリティプログラム３０５は、ディジタル署名の検証を行う（ステップ４２０）。ディジタル署名が正しく検証できなかった場合には、サービス利用プログラム３０３は、検証失敗メッセージをサービス提供者装置１００に送信し（ステップ４２１）、正しく検証できた場合には、署名付時刻保証データに含まれている時刻情報の妥当性を確認した後、該署名付時刻保証データを、記憶装置２０６内に保存済みの前記時刻保証依頼用データと関連付けて記憶装置２０６に保存する。署名付時刻保証データは、署名処理装置２０７に追記されるようにしても良い。

【００７９】時刻情報が所定の基準から外れる等の理由により、妥当性に欠けるものであったならば、当該署名付時刻保証データを破棄するとともに、ステップ４００から再度行う。上記基準は、通常の応答時間、許容できる遅れ時間などに基づいて設定すればよい。

【００８０】サービスの利用をやめる場合には、そのまま処理を終了してもよい。サービス提供者装置１００が検証失敗メッセージを受け取った場合には、当該署名付時刻保証データを利用者装置１１０$_1$に再送する。

【００８１】ステップ４０７において、利用者装置１１０$_2$を選択する方法として、同じような証明を依頼してきた他の利用者装置の中から選ぶようにしても良い。複

数の利用者装置を選んでも良く、その場合は、ステップ４１５以降について、選択数にあわせた回数を実施する。

【００８２】上述の操作を行なうことにより、作成した時刻保証依頼用データは、他の利用者によってその作成時刻が保証される。この操作を、時刻保証を必要とする処理の前または後あるいは両方に行なえば、その前後関係が保証される。

【００８３】例えば、図５の１６番に示す「Ｆとの電子契約文書」の作成時刻保証を必要とする場合には、作成時の前後に、時刻保証依頼用データを作成して保証してもらい、１５番から１８番に一連の署名履歴を格納すれば、作成時刻がある程度の時間をもって保証される。

【００８４】利用者装置1102も、図５の１７、１９、３２番のように、利用者装置1101のために作成した署名付き時刻保証データを、自らの装置が作成した時刻保証依頼用データと混在させて、署名履歴のなかに残すことになる。そして、図４に示すディジタル署名を検証するステップ４０９で、依頼者を特定する情報を得ることが出来るので、これをたとえば記憶装置２０６に保存しておき、後の調停作業での問い合わせに使うことにより、他の利用者装置のために行なった署名の履歴も時刻保証用として用いることが可能になる。たとえば１６番の「Ｆとの電子契約文書」の作成時刻が、１５番と１７番の履歴により、より狭い範囲で保証されるようになる。

【００８５】記憶装置２０６に保存した、時刻保証依頼用データとそれに関連付けられた署名付時刻保証データとは、後に、調停が必要になったときの証明に必要になるものなので、失われないように定期的にバックアップデータを作成するか、不揮発性の記憶装置に保存するなどの処理を行なうことが望ましい。

【００８６】次に、本実施形態のネットワークサービスシステムにおいて、利用者間で過去に取り交わした電子契約文書にディジタル署名を施した日時を確認する方法について、図面を参照して説明する。

【００８７】図６は、調停者が調停作業を行う場合の調停者装置６００の動作を説明するための図である。調停者が使用する調停者装置６００は、基本的に図２に示すサービス提供者装置１００と同様の構成である。ただし、利用者装置１１０の記憶装置２０６に格納された時刻保証依頼用データや署名付時刻保証データ、あるいは署名処理装置２０７に格納された署名履歴などを、途中で改ざんされないように暗号化した状態で入手したり、ネットワークを用いないより安全な経路で入手する手段を備える。

【００８８】該調停者装置６００のソフトウェア構成は基本的に図３（ａ）に示すサービス提供者装置１００のソフトウェア構成と同様である。ただし、サービス提供プログラム３０２の代わりに、図６に示す調停作業を制御するための調停プログラム３０６（図示せず）が記憶されている点が異なっている。

【００８９】調停プログラム６００は、当該電子契約文書に署名した各利用者の署名処理装置２０７から署名履歴を入手する（ステップ６０１）。該電子契約文書に関する情報が署名履歴に含まれているかどうかを確認し（ステップ６０２）、含まれていなければ該電子契約文書は誰かによって偽造されたものと判定する（ステップ６０３）。

【００９０】電子契約文書に関する情報が署名履歴に含まれていた場合、調停プログラム３０６は、該署名履歴を検索し、該電子契約文書の前後一番時刻が近い、時刻保証依頼用データへの署名履歴（それぞれ前時刻保証データおよび後時刻保証データという）を探す（ステップ６０４）。例えば、図５において、１６番の電子契約文書の前時刻保証データは１５番であり、後時刻保証データは１８番である。３３番の電子契約文書の前時刻保証データは３１番であり、後時刻保証データは３５番である。前時刻保証データおよび後時刻保証データを選択できなければ、署名時刻を特定不可能として処理を終了する（ステップ６１３）。１７番の署名付き時刻保証依頼用データを１８番の代わりに用いても良いし、３２番の署名付き時刻保証依頼用データを３１番の代わりに用いても良い。

【００９１】調停プログラム３０６は、利用者装置1101が具備する記憶装置２０６から時刻保証依頼用データと署名付時刻保証データとを入手し（ステップ６０５）、該データの中に、上記前時刻保証データおよび後時刻保証データに対応する署名付時刻保証データがそれぞれ含まれているかどうかを確認する（ステップ６０６）。該当するデータがなければ、前記動作手順において、署名付時刻保証データが正しく生成されなかったと判定し（ステップ６０７）、署名履歴の中から次に近い位置にある前時刻保証データおよび後時刻保証データを選択しなおす（ステップ６０８）。さらに、選択可能な前時刻保証データおよび後時刻保証データがなければ、署名時刻を特定不可能として処理を終了する（ステップ６１３）。

【００９２】調停プログラム３０６は、該当する署名付き時刻保証データがあれば、その署名から上記二つの署名付時刻保証データを生成した利用者の署名処理装置２０７を特定し、署名履歴をそれぞれ入手する（ステップ６０９）。上述のように、サービス提供者装置は、時刻保証依頼データを送る利用者装置１１０を、一定にしないので、それぞれの署名付き時刻保証データを生成した署名処理装置２０７から署名履歴を入手する。署名履歴を生成した署名処理装置２０７は、当該署名から特定することができる。

【００９３】調停プログラム３０６は、該署名履歴の中に、当該署名付時刻保証データに対応した情報がそれぞ

れ含まれているかどうかを確認する（ステップ６１０）。該署名付時刻保証データに関する情報が署名履歴に含まれていなければ、該署名付時刻保証データは誰かによって偽造されたものと判定し（ステップ６１１）、署名時刻を特定不可能として処理を終了し（ステップ６１３）、含まれていれば、当該電子契約文書は、前時刻保証データおよび後時刻保証データに含まれる時刻情報の間にディジタル署名が施されたと判断する（ステップ６１２）。

【００９４】調停プログラム３０６は、図６の各ステップで必要に応じて署名の正当性を検証し、確認できなければ署名が偽造されたものと判断する。

【００９５】上記手順は、調停者に依頼せずに関係者間で調停作業を行う場合も同様である。

【００９６】上記の本実施形態によれば、サービス提供者装置は、自ら署名することが無く、システム全体の安全性に影響するような秘密情報を管理することがないので、より安全である。また、一つ一つに署名するという負荷がかからず、簡単な手順で運用することができるので、サービス提供時の処理速度が低下するおそれが少ない。

【００９７】本発明によれば、サービス提供者装置に依存することなく、複数の利用者が相互に協力することによって、利用者がディジタル署名を施した時刻を保証する方法とそれを用いたサービスが実現できる。

【００９８】本実施形態では、上記実施例以外にも氏名や住所などといった利用者の属性情報または所有物に関する情報や、公開鍵や特許アイデアなどといった利用者の所有物、あるいは、申請や契約などといった利用者の行為などを保証するデータ、または、上記電子契約文書そのものなど、あらゆるマルチメディアデータを時刻保証用依頼データとして用いることができる。この場合、依頼データそのものがその時点で存在したという証明を他の利用者に行ってもらうことができる。時刻保証依頼用データとして、それらをハッシュ関数によって圧縮した特徴値（ハッシュ値）などを用いてもよい。さらに、上記のいずれか一つであってもよいし、それらの組み合わせであってもよい。

【００９９】本発明で用いられるハッシュ関数としては、安全性を確保する目的からは、同じ出力値を与えるような２つの異なる入力値を見出すことと、出力がある与えられた値となる入力値を見出すこととが困難であるような関数を用いることが望ましい。ハッシュ関数のアルゴリズムはシステム全体に対して公開されているものとする。

【０１００】この変形例のように、依頼データそのものの存在を証明してもらう場合に時刻証明が必須ではない場合は、時刻情報を含めずに署名してもらうようにしてもよい。

【０１０１】時刻情報をサービス提供者装置１００が署名なしの状態で付加するようにしてもよいし、利用者装置１１０_{1}が時刻保証依頼用データの中に含めるようにしてもよい。この場合でも、時刻情報が付加されたデータを受け取ったそれぞれの装置では、その正当性、妥当性を確認した上でそれぞれの処理を進めるようにすれば、より信頼性が高まる。

【０１０２】本実施形態では、時刻保証依頼用データとして、ランダムに生成したものではなく、それ以前の署名履歴などを用いれば、署名履歴自体の信頼性も高まる。

【０１０３】上記実施形態とは異なり、ある利用者端末からのサービス提供依頼を受けたら、該依頼を、次にサービス提供依頼を送ってきた利用者端末に送るようにしてもよい。このようにすれば、各利用者端末がサービスを受ける際には、その前にサービス提供者装置からの依頼を処理することが必要となるため、該サービス提供者装置からの依頼が正しく処理されるケースが増加するものと考えられる。

【０１０４】本実施例では、サービス提供者１３０は、本発明のネットワークサービスシステムの利用者が信頼する第三者であり、不正行為を働くことはないものと仮定している。また、利用者１４０は、システムを利用する一般の人であり、少数の利用者は利益を得るためなどの目的により不正行為を働く可能性がある。

【０１０５】不正行為を働く少数の利用者による影響を排除するため、利用者装置１１０を除く複数の利用者装置をランダムに選んで、それぞれに対して署名時刻保証依頼データを送信し、返信されてきた署名時刻保証データを、利用者装置１１０に送るようにしてもよい。このようにすれば、一つまたは少数の利用者端末を操作する利用者が不正行為を働いたとしても、それ以外の多くの利用者端末から正しく処理された署名時刻保証データが返送されてくることが期待でき、処理が滞る危険性が減る。

【０１０６】また、利用者間の結託を考慮する必要がなければ、本実施形態とは異なり、利用者だけで同様の処理を行ってもよい。

【０１０７】（実施例２）本発明の第二の実施形態が適用されたネットワークサービスシステムの概略構成と、システムを構成するサービス提供者装置１００および利用者装置１１０のハードウェア構成、ソフトウェア構成は、図１から図３と同様である。

【０１０８】本実施形態で用いる署名時刻保証方法の手順について、図面を参照して説明する。以下の例も、実施例１と同様、各利用者が利用者装置を操作し、他の利用者との間でディジタル署名を施した電子契約文書をやり取りする個々の契約手続きの合間に、この署名時刻保証方法を利用することにより、個々の契約手続が行なわれた時刻を証明するものである。

【０１０９】図７は、利用者１４０が、サービス提供者

１３０が提供するサービスを受ける場合の、サービス提供者装置１００、および利用者装置１１０の動作を説明するための図である。

【０１１０】サービス提供者装置１００において、サービス提供プログラム３０２は、有効期間（締め切り）を設定したチャレンジデータを所定の規則に従うかあるいはランダムに生成し（ステップ７００）、該チャレンジデータを、各利用者装置１１０がネットワークを介して読み取り可能な状態で公開する（ステップ７０１）。

【０１１１】ここでは、有効期間を１日とし、次の日になるまで公開するものとする。

【０１１２】利用者装置１１０において、サービス利用プログラム３０３は、サービス提供者装置１００が公開しているチャレンジデータを、ネットワークを介して取得し（ステップ７０２）、セキュリティプログラム３０５を用いて該チャレンジデータにディジタル署名を施し（ステップ７０３）、署名処理装置２０７に設けた署名履歴の中に、該チャレンジデータとそのディジタル署名を追記する（ステップ７０４）。サービス利用プログラム３０３は、当該署名付チャレンジデータをサービス提供者装置１００に送信する（ステップ７０５）。

【０１１３】図５に示す署名履歴では、時刻保証依頼用データの代わりにチャレンジデータが署名対象データとして記憶される。

【０１１４】サービス提供者装置１００において、サービス提供プログラム３０２は、署名付チャレンジデータを受信する（ステップ７０６）。サービス提供プログラム３０２は、受信時刻が締切時刻を過ぎていないかどうかを確認し、締め切りを過ぎていた場合には、締切過ぎのため受付できない旨の締切過ぎメッセージを利用者装置１１０に送信する（ステップ７０７）。締切時刻以前の場合には、受信した署名付チャレンジデータに施されているディジタル署名の検証を行い、ディジタル署名が正しく検証できなかった場合には、サービス提供プログラム３０２は、検証失敗メッセージを利用者装置１１０に送信する（ステップ７０９）。正しく検証できた場合には、当該署名付チャレンジデータを記憶装置２０６に保存し（ステップ７１１）、受付完了メッセージを利用者装置１１０に送信する（ステップ７１２）。利用者装置１１０において、サービス利用プログラム３０３は、送られた受付完了メッセージを受信する（ステップ７１３）。

【０１１５】サービス提供者装置１００は、利用者からその日のうちに（有効期間内に）送信されてきた署名付チャレンジデータを、例えば図８のように、当該チャレンジデータを公開した日やチャレンジデータと組にして、記憶装置２０６に記憶する。ステップ７０９の検証処理は省略してもよく、その場合には後述の調停処理で署名の検証を行う。

【０１１６】上記ステップにおいて、利用者装置１１０が締切過ぎメッセージ（ステップ７０８）や検証失敗メッセージ（ステップ７１０）を受け取った場合には、ステップ７０２から再度行っても良いし、そのまま処理を終了してサービスの利用をやめてもよい。

【０１１７】利用者装置１１０において、サービス利用プログラム３０３は、取得したチャレンジデータを記憶装置２０６にも格納し、受け取った受付完了メッセージを、格納したチャレンジデータと関連づけて記憶装置２０６に格納するようにしても良い。サービス提供者装置１００が複数あって、いずれかのチャレンジデータを選択した場合などは、いずれのサービス提供者装置１００であるかを特定する情報を併せて格納すると、調停作業により有効である。

【０１１８】次に、本実施形態のネットワークサービスシステムにおいて、利用者間で過去に取り交わした電子契約文書にディジタル署名を施した日時を確認する方法について、図面を参照して説明する。

【０１１９】図９は、調停者が調停作業を行う場合に使用する調停者装置６００の動作を説明するための図であり、調停者装置６００の構成は、実施例１の場合と同様である。

【０１２０】図９において、６０１から６０３は、実施例１と同様の処理を行うステップであり、図６と同じ番号を付している。

【０１２１】ステップ６０２において、電子契約文書に関する情報が署名履歴に含まれていた場合、調停プログラム３０６は、図６のステップ６０４と同様に、前時刻保証データおよび後時刻保証データとして、チャレンジデータへの署名履歴を探す（ステップ９０１）。前時刻保証データおよび後時刻保証データを選択できなければ、署名時刻を特定不可能として処理を終了する（ステップ６１３）。

【０１２２】調停プログラム３０６は、サービス提供者装置１００が具備する記憶装置２０６に保存された署名付チャレンジデータを入手し（ステップ９０２）、その一覧の中に、上記前時刻保証データおよび後時刻保証データが、含まれているかどうかを確認する（ステップ９０３）。該当するデータが記憶装置２０６に、署名付チャレンジデータとして保存されていなければ、前記動作手順において、締切りを過ぎてから署名付チャレンジデータを送信した、あるいは署名付チャレンジデータが正しく生成されなかった、のいずれかであると判定し（ステップ９０４）、署名履歴の中から次に近い位置にある前時刻保証データおよび後時刻保証データを選択しなおす（ステップ９０５）。選択可能な前時刻保証データおよび後時刻保証データがなければ、署名時刻を特定不可能として処理を終了する（ステップ６１３）。

【０１２３】ステップ９０３において、上記前時刻保証データおよび後時刻保証データが署名付チャレンジデータに含まれているならば、調停プログラム３０６は、例

えば、図５の１６番の電子契約文書の場合には２０００年２月２０日にディジタル署名が施されたと判断し、３３番の電子契約文書の場合には２０００年３月１日から２０００年３月３日のいずれかの日にディジタル署名が施されたと判定する（ステップ６１２）。

【０１２４】調停プログラム３０６は、図９の各ステップで必要に応じて署名の正当性を検証し、確認できなければ署名が偽造されたものと判断する。

【０１２５】上記手順は、調停者に依頼せずに関係者間で調停作業を行う場合も同様である。

【０１２６】上記の本実施形態によれば、サービス提供者装置は、システム全体の安全性に関わるような秘密情報を管理することがないので、より安全である。また、負荷の少ない簡単な手順で運用することができるので、サービス提供時の処理速度が低下するおそれが少ない。

【０１２７】本発明によれば、サービス提供者装置に依存することなく、利用者がディジタル署名を施した時刻を保証する方法とそれを用いたサービスが実現できる。

【０１２８】本実施形態におけるチャレンジデータは、時単位や分単位などで変更するようにしてもよい。

【０１２９】本実施形態では、電子契約文書の作成時に、その時点で公開されているチャレンジデータを取得し、該電子契約文書（あるいはそのハッシュ値などの特徴値）とチャレンジデータとを連結したものに署名を施して、サービス提供者装置に送信するようにしてもよい。このようにすることにより、署名時刻をより詳細に特定できるようになる。

【０１３０】利用者装置が締切過ぎメッセージや検証失敗メッセージを受け取って最初からやり直す場合に、該締切過ぎメッセージや検証失敗メッセージと対応する署名履歴にその旨を示す識別子を追記するようにしてもよい。このようにすることにより、ディジタル署名を施した時刻を確認する際の手間が軽減される。

【０１３１】サービス提供者装置を複数に分け、チャレンジデータの公開と署名付チャレンジデータの保存とを、別々の装置で行うようにしてもよい。

【０１３２】上記各実施形態におけるディジタル署名には、検証作業に必要な、署名者を特定する情報か、検証に必要な公開鍵が添付されているものとする。サービス提供者装置１００や利用者装置１１０や調停者装置６００において、検証を行う各プログラムは、署名に添付されている情報を元に、認証局から公開鍵を入手したり、公開鍵の証明書を入手したりする。

【０１３３】上記各実施形態において、前時刻保証データまたは後時刻保証データいずれか一方があれば目的を達成する場合もあり得る。状況に応じて運用することが可能である。

【０１３４】上記各実施形態において、サービス提供者装置が利用者装置の機能を兼ね備えており、利用者は、利用者装置に導入したアクセスプログラム（ブラウザなど）を操作し、ネットワークを介してサービス提供者装置にアクセスし、該サービス提供者装置が具備する機能を使って、署名付時刻保証依頼用データや署名付時刻保証データ（実施例１の場合）、あるいは署名付チャレンジデータ（実施例２の場合）を生成するようにしてもよい。その場合は、サービス提供者装置側に、上記アクセス時に個々の利用者を識別するための認証機能や、その結果にしたがったアクセス制御機能、署名生成・検証機能、署名履歴保存機能などを設ければよい。

【０１３５】上記各実施形態において、利用者装置１１０において本発明によるシステムを実現するのに必要な各プログラムは、サービス提供者装置１００またはその他のサーバからネットワーク経由で事前に、または必要なときにダウンロードするようにしても良い。または、ＣＤＲＯＭ、ＦＤなどの可搬型記憶媒体を経由して導入されるようにしても良い。

【０１３６】

【発明の効果】本発明によれば、より高い安全性を持つ情報の正当性の保証方法、または、サービス提供者の負荷も少ない情報の保証方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の実施例１および実施例２が適用されたネットワークサービスシステムの概略構成図である。

【図２】サービス提供者装置１００および利用者装置１１０のハードウェア構成を示す図である。

【図３】サービス提供者装置１００および利用者装置１１０が具備するメモリ２０４のソフトウェア構成を示す図である。

【図４】本発明の実施例１において、利用者１４０が、サービス提供者１３０が提供するサービスを受ける場合の、サービス提供者装置１００、利用者装置１１０_{1}、および利用者装置１１０_{2}の動作を説明するためのフロー図である。

【図５】利用者装置１１０が具備する署名処理装置２０７に保存される署名履歴の一例を示す図である。

【図６】本発明の実施例１において、調停者が調停作業を行う場合の調停プログラム３０６の動作を説明するためのフロー図である。

【図７】本発明の実施例２において、利用者１４０が、サービス提供者１３０が提供するサービスを受ける場合の、サービス提供者装置１００、および利用者装置１１０の動作を説明するためのフロー図である。

【図８】サービス提供者装置１００が具備する記憶装置２０６に保存される署名付チャレンジデータ等の一例を示す図である。

【図９】本発明の実施例２において、調停者が調停作業を行う場合の調停プログラム３０６の動作を説明するためのフロー図である。

【図１０】本発明の実施例１において、各利用者の署名履歴が交差した場合の一例を示す図である。

27

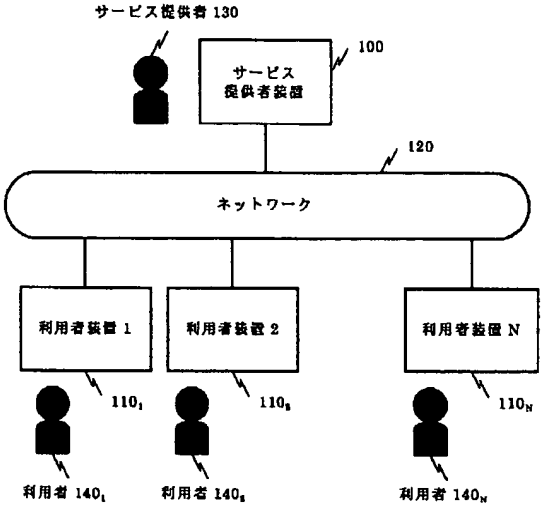
【符号の説明】

１００…サービス提供者装置、１１０…利用者装置、１３０…サービス提供者、１４０…利用者、２０６…記憶装置、２０７…署名処理装置、３０２…サービス提供プログラム、３０３…サービス利用プログラム、３０４…電子文書処理プログラム、３０５…セキュリティプログラム、６００…調停者装置。

28

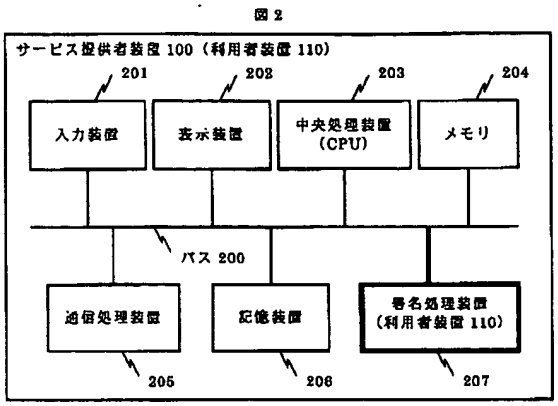
【図１】

図１



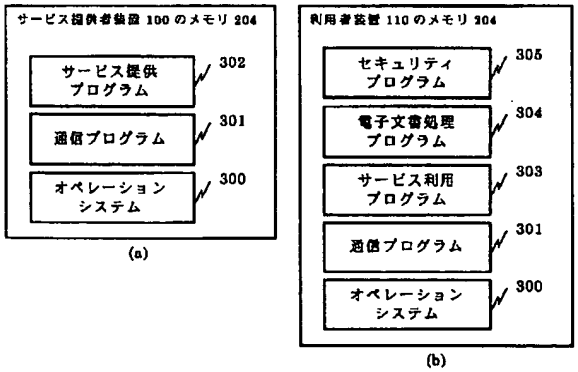
【図２】

図２



【図３】

図３



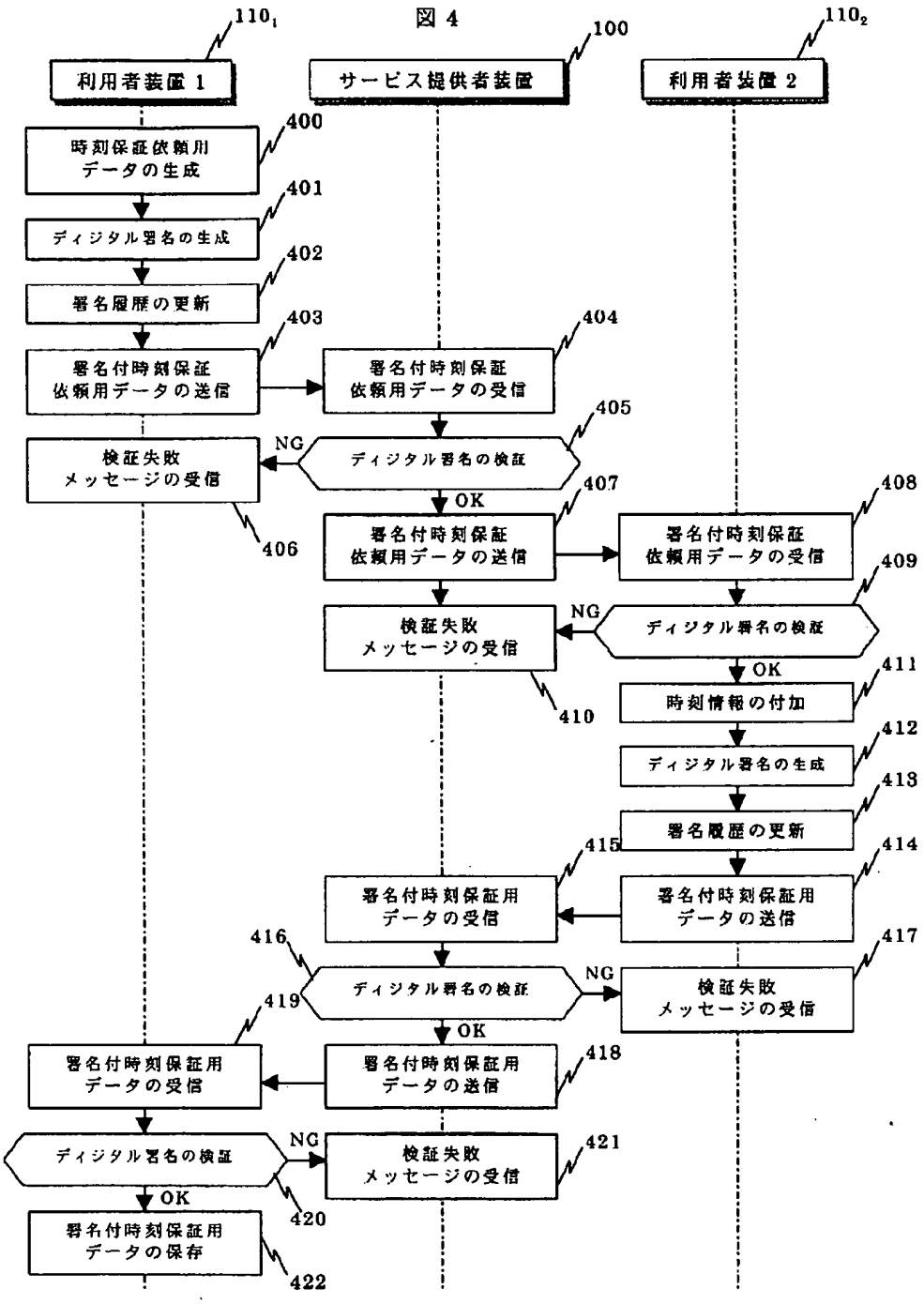
【図５】

図５

通番	署名対象データ	署名データ	
1	Ａとの電子契約文書	**********	
2	Ｂとの電子契約文書	**********	
3	時刻保証依頼用データ１	**********	
4	Ｂとの電子契約文書	**********	
:	:	:	
15	時刻保証依頼用データ２	**********	（前時刻保証データ）
16	Ｆとの電子契約文書	**********	
17	署名付時刻保証依頼用データ１	**********	（署名付き時刻保証データ）
18	時刻保証依頼用データ３	**********	（後時刻保証データ）
19	署名付時刻保証依頼用データ２	**********	（署名付き時刻保証データ）
20	Ｄとの電子契約文書	**********	
:	:	:	
31	時刻保証依頼用データ４	**********	
32	署名付時刻保証依頼用データ３	**********	
33	Ａとの電子契約文書	**********	
34	Ｄとの電子契約文書	**********	
35	時刻保証依頼用データ５	**********	
:	:	:	

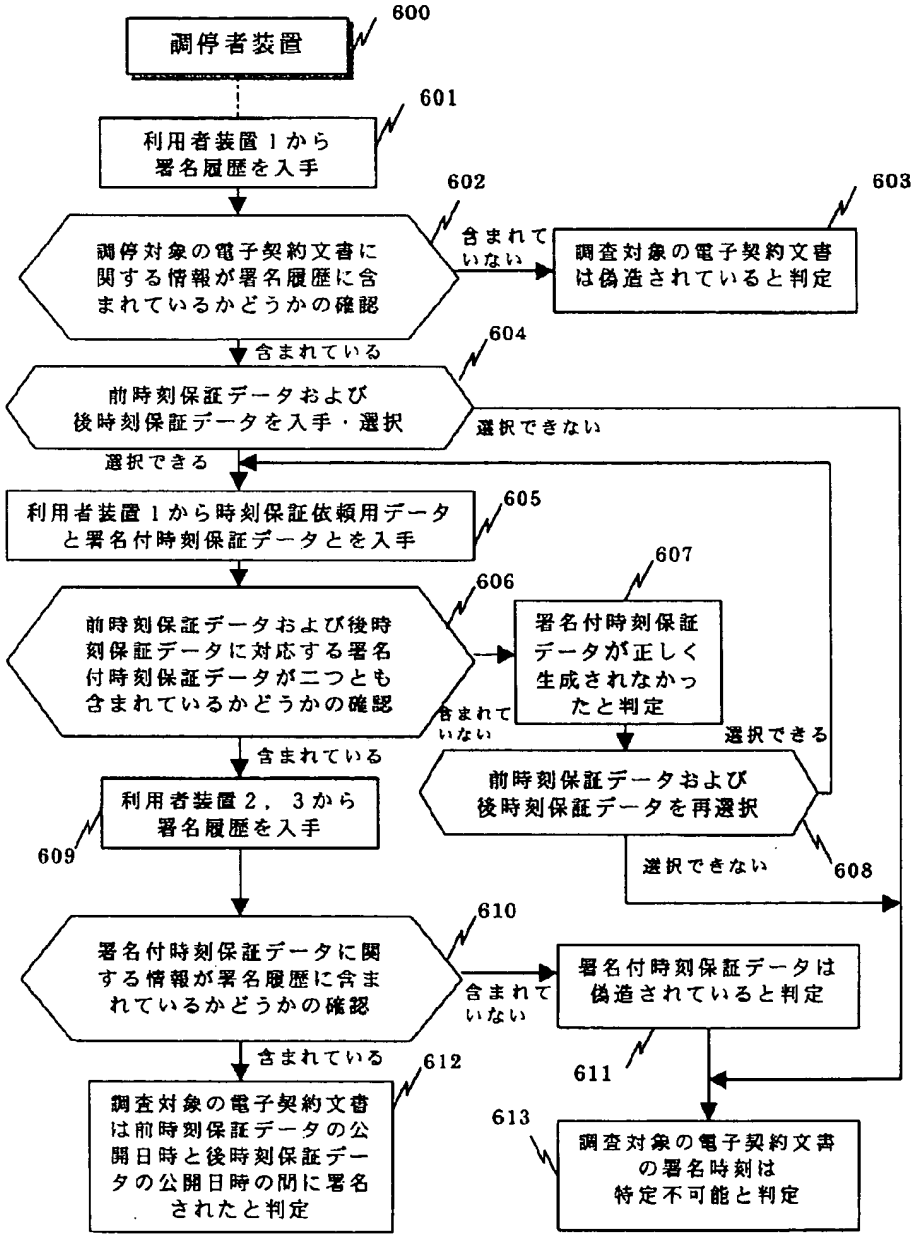
【図４】

図 4


110_1
利用者装置 1
100
サービス提供者装置
110_2
利用者装置 2
400
時刻保証依頼用データの生成
401
ディジタル署名の生成
402
署名履歴の更新
403
署名付時刻保証依頼用データの送信
404
署名付時刻保証依頼用データの受信
405
ディジタル署名の検証
NG
検証失敗メッセージの受信
406
OK
407
署名付時刻保証依頼用データの送信
408
署名付時刻保証依頼用データの受信
409
ディジタル署名の検証
NG
検証失敗メッセージの受信
410
OK
411
時刻情報の付加
412
ディジタル署名の生成
413
署名履歴の更新
414
署名付時刻保証用データの送信
415
署名付時刻保証用データの受信
416
ディジタル署名の検証
NG
417
検証失敗メッセージの受信
OK
418
署名付時刻保証用データの送信
419
署名付時刻保証用データの受信
ディジタル署名の検証
NG
421
検証失敗メッセージの受信
420
OK
署名付時刻保証用データの保存
422

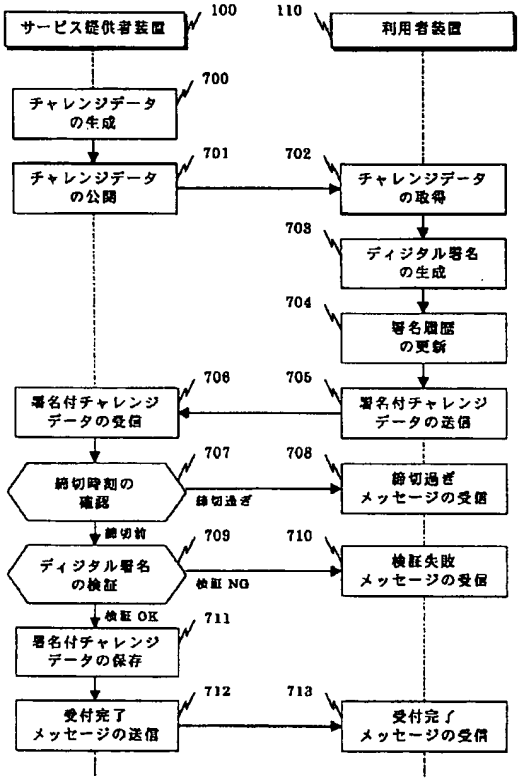
【図６】

図６


調停者装置
600
利用者装置１から署名履歴を入手
601
調停対象の電子契約文書に関する情報が署名履歴に含まれているかどうかの確認
602
含まれていない
調査対象の電子契約文書は偽造されていると判定
603
含まれている
前時刻保証データおよび後時刻保証データを入手・選択
604
選択できない
選択できる
利用者装置１から時刻保証依頼用データと署名付時刻保証データとを入手
605
前時刻保証データおよび後時刻保証データに対応する署名付時刻保証データが二つとも含まれているかどうかの確認
606
署名付時刻保証データが正しく生成されなかったと判定
607
含まれていない
選択できる
含まれている
利用者装置２，３から署名履歴を入手
609
前時刻保証データおよび後時刻保証データを再選択
608
選択できない
署名付時刻保証データに関する情報が署名履歴に含まれているかどうかの確認
610
含まれていない
署名付時刻保証データは偽造されていると判定
611
含まれている
調査対象の電子契約文書は前時刻保証データの公開日時と後時刻保証データの公開日時の間に署名されたと判定
612
調査対象の電子契約文書の署名時刻は特定不可能と判定
613

【図７】

図７



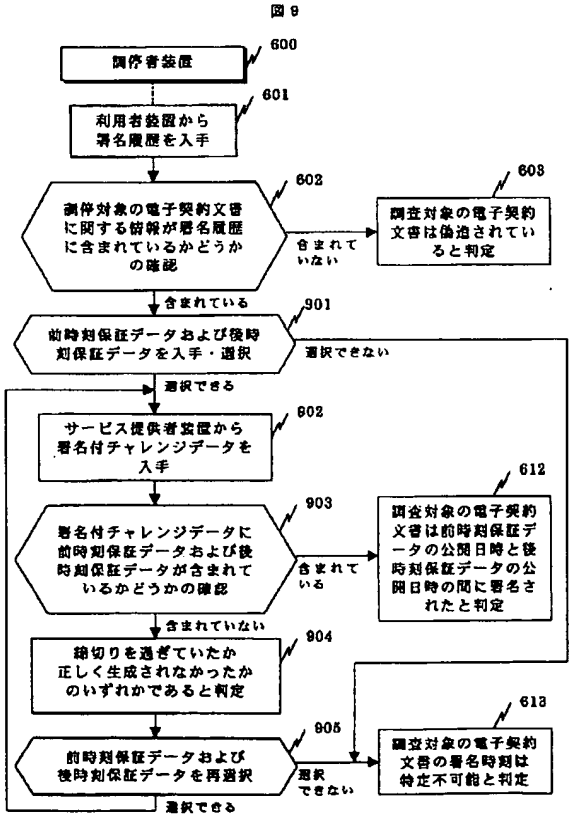
【図８】

図８

公開日時	チャレンジデータ	署名付チャレンジデータ
2000年1月1日	**********	利用者5のデータ
		利用者12のデータ
		利用者1のデータ
		⋮
2000年1月2日	**********	利用者2のデータ
		利用者1のデータ
		利用者9のデータ
		⋮
⋮	⋮	⋮

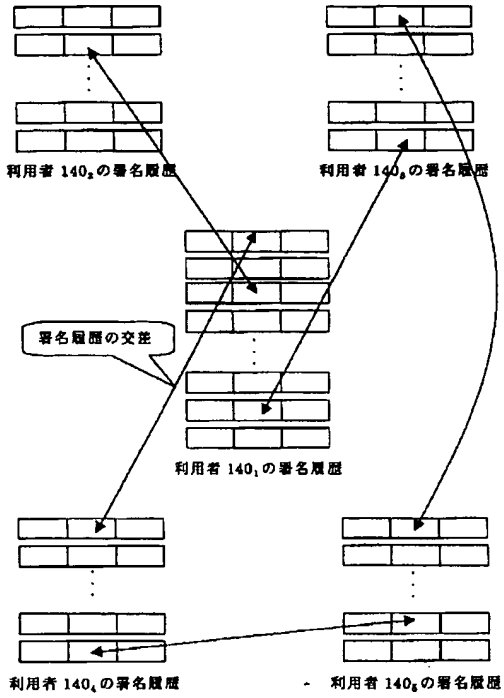
【図９】

図９



【図１０】

図 10



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　19/00	１４０	Ｇ０６Ｆ　19/00	１４０

(72)発明者　佐々木　良一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　松木　武
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報サービス事業部内
(72)発明者　竹内　国人
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所金融システム事業部内
(72)発明者　岩村　充
東京都練馬区中村２－14－17
(72)発明者　松本　勉
神奈川県横浜市青葉区柿の木台13－45

Ｆターム(参考)　5B017 AA07 BA07 CA16
5B049 BB00 CC02 CC31 DD00 EE03 EE09 FF03 FF04 GG04 GG07 GG10
5J104 AA09 AA11 BA02 JA21 LA03 LA06 NA12